United States Army Signal Center, Fort Gordon, Georgia
Leader College of Information Technology

Simple Network Management Model (SNMM)

93d Signal Brigade Data Package
Network Management Model

Functional Area 24 Telecommunications Systems Engineer Course Class 02-01

Kenneth Lawrence, Billy L. Miller, Paul Powell
kenneth.lawrence@us.army.mil billy.miller@us.army.mil paul.powell@us.army.mil

28 May 2002

Table of Contents

Simple Network Management Model
93D Signal Brigade Data Package

Billy L. Miller, Kenneth L. Lawrence, Paul Powell
billy.miller@us.army.mil kenneth.lawrence@us.army.mil paul.powell@us.army.mil

1. Introduction

The Simple Network Management Model (SNMM) demonstrates how network management systems (NMS) functions in support of the 93rd Signal Brigade's Data Packages. The 93rd Signal Brigade has developed an integrated C4 Package in support of its increasing data communications requirements. Commercial-off-the-Shelf (COTS) equipment has become commonplace in the United States Armed Forces communications networks. This co-occupancy between COTS and military hardware and software technology has allowed increased capabilities for users in tactical environments. However, it has also created a myriad of problems in the realm of network management. Does COTS and military devices have the same protocols for communications and management? The answer to that question is one of the focuses of this project.

The goal of network management is to fulfill the requirements of both the owners and users of the network. To meet this goal, industry standards associated with COTS equipment must be incorporated and utilized within military communication networks. Standards organizations, such as the International Telecommunications Union (ITU), Internet Engineering Task Force (IETF) and the International Standards Organization (ISO), have created internationally accepted protocols for communication between similar systems made by different vendors.

By acceptable definition, network management is described as "the techniques concentrated on managing hardware devices (modems, routers, multiplexers, network interfaces, and connections)."[11]The Army has recognized the magnitude and the essential need for network management to effectively and efficiently optimizes the Army's critical information technology business processes. Per Field Manual 6-02.71, " … to enable Army Signal Commanders J6/G6s to provide optimal communications support to users conducting the Army's operational mission."[2] To gain a better understanding of the 93rd Signal Brigade's deployable C4 Packages, in terms of a network management model, this project will lay the foundation for establishing tools for network management of strategic and tactical systems.

2. Background

The Tactical Packet Network (TPN), X.25, was the Army Signal Corps answer to growing data communications demands from warfighters throughout the Army. TPN was created as an after thought of voice communications. For a long time in the telecommunications industry voice communications was the standard that defined the design of communication networks. TPN deleted voice channels; it had a low data rate (16kbps) and it had dissimilar user-to-network protocols. With growing data

[1]

communications requirements, the Army Signal Commands had to find a solution, fast!! First, the bandwidth capacity[2] for Mobile Subscriber Equipment and Digital Group Multiplexer Equipment was improved with the Tactical High-Speed Data Network (THDSN) upgrade. Another improvement made by U.S. Army Commands around the world was the creation of user data packages. The 93rd Signal Brigade under the Army Signal Command (ASC) decided to assembly some COTS and military software and hardware products together into a data package. Thus, the data packages were created.

2.1 Overview of the 93rd Signal Brigade

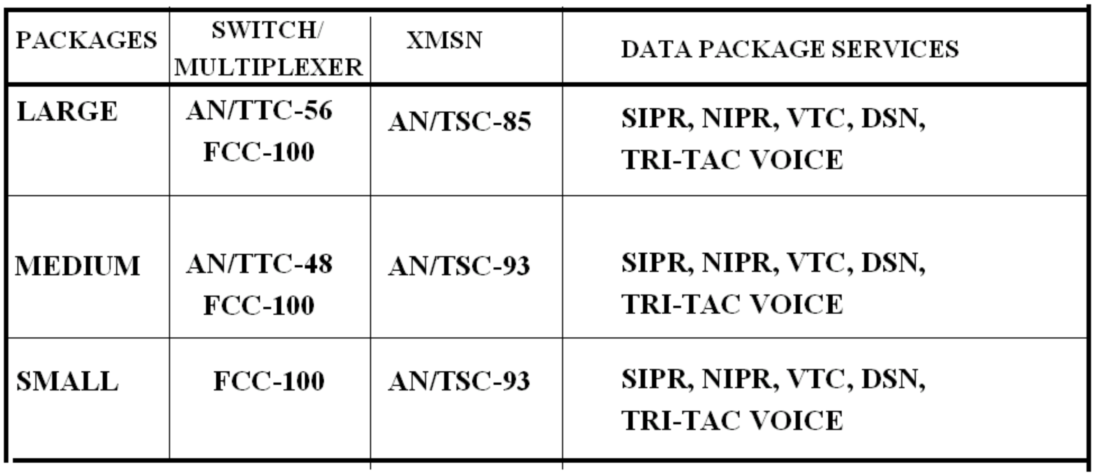
The 93rd Signal Brigade is rapid deployable tactical signal unit, a subordinate organization of Army Signal Command (ASC). The echelons above corps unit provide digital voice and data communications to common users. The brigade utilizes Digital Group Multiplexer (DGM) equipment consisting of: Node Centers providing tandem trunk switching, Large Extension Nodes (LEN) providing intermediate access, and Small Extension Nodes (SEN) providing remote access. Inter-nodal connectivity is being provided by line-of-sight transmissions (LOS), tactical satellite and cable equipment. The unit's mission is to deploy, install, operate, and maintain a tactical theater communications package worldwide while supporting joint and combined operations. Legacy DGM equipment has not been able to meet the increasing demands for data communications. The Army has recognized this increase in requirements for data and video users in tactical and strategic areas of operations. The Warfighter Information Network-Tactical (WIN-T) is the Army's tactical solution to DGM and Mobile Subscriber Equipment (MSE) to meet those requirements. Unfortunately, WIN-T has not been fully implemented in the field. The 93rd Signal Brigade designed and implemented data communications packages to meet the data and video requirements of its subscribers. Advances in commercial telecommunications technology have allowed the integration of COTS and legacy military equipment.

The brigade's need for data communications packages led to Headquarters Department of the Army approval for the 518th Theater Installation Network (TIN) Company. The 518th TIN Company has nine deployable data packages located at Fort Gordon, Georgia in support of worldwide operations. The 93rd Signal Brigade deploys data packages with each tactical satellite terminals and switches. The brigade refers to equipment composites as "C4 Packages". These C4 packages are a composite of tactical switches, tactical satellite and data packages that will be deployed in tactical or strategic areas of operations in support of warfighting commanders. Tactical satellite terminals provide long haul connectivity through Strategic Tactical Entry Point (STEP) sites and Defense Satellite Communications System (DSCS) terminals with reach back to the 93rd Signal Brigade's Theater Network Operations Security Center (TNOSC). The brigade

[1] Smith, Marina: "Virtual LANS", McGraw Hill, New York, 1998.

[2] Network Management, Telecom Systems Engineer Course, FA24 Lecture Notes.

deploys these C4 packages in three ready, rapid and deployable elements. The 93rd Signal Brigades C4 Packages are model in three facets, Large C4 Package, Medium C4 Package and Small C4 Package, as illustrated in Figure 1.



PACKAGES	SWITCH/ MULTIPLEXER	XMSN	DATA PACKAGE SERVICES
LARGE	AN/TTC-56 FCC-100	AN/TSC-85	SIPR, NIPR, VTC, DSN, TRI-TAC VOICE
MEDIUM	AN/TTC-48 FCC-100	AN/TSC-93	SIPR, NIPR, VTC, DSN, TRI-TAC VOICE
SMALL	FCC-100	AN/TSC-93	SIPR, NIPR, VTC, DSN, TRI-TAC VOICE

Figure 1. 93rd Signal Brigade's Deployment Strategies for C4 Data Packages

2.2 Overview of the Data Package

The 93rd Signal Brigade's data package is an assembly of procured COTS equipment. These rapid contingency data packages deploy into theaters and areas of operations along with tactical satellite terminals and switches to provide point of presence (POP) insertion. Users are granted access to the Defense Information Systems Network (DISN) cloud, which is synonymous to the commercial wide area network (WAN). Data packages have the capability of supporting 300 data service clients per terminal in a seamless strategic and tactical environment. The myriad of services provided to customers is Non-Secure Internet Protocol Network (NIPR), Secure Internet Protocol Network (SIPR), Defense Switched Network (DSN), Video Teleconference and TRI-TAC Voice. The COTS equipment is packaged in a mobile rack mountable carrying case, consisting of three cases as illustrated Figure 2. The first case contains the transmission/multiplexing equipment. The second and third cases contain the NIPR and SIPR data services suites respectively.

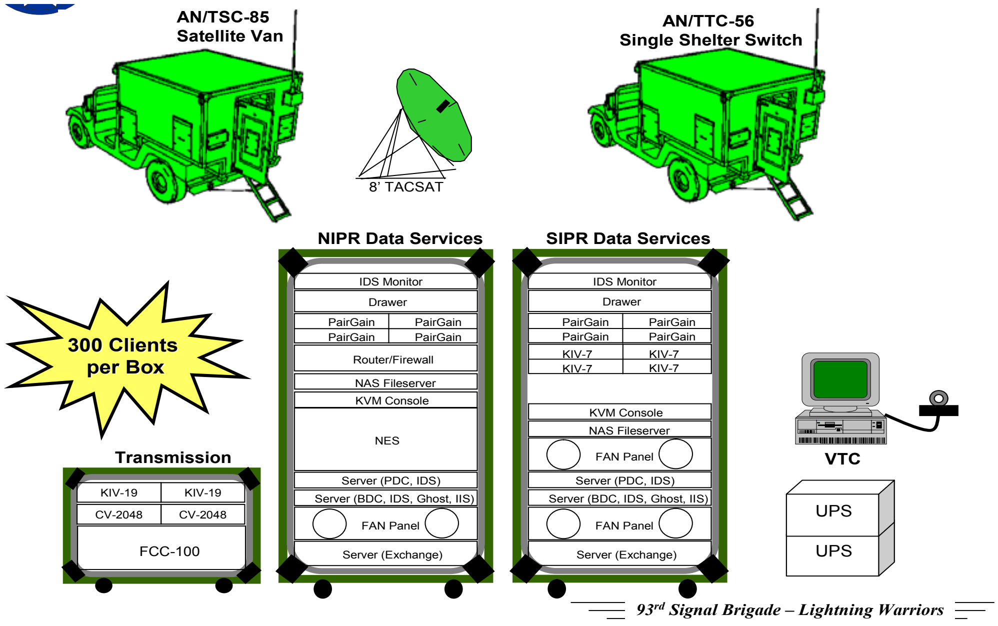


Figure 2. Data Services Package

2.3 Data Package Component List Breakdown

The data package architecture is a mixture of legacy and COTS equipment. The COTS equipment is not vendor specific. The legacy and COTS components each serve specific functions as illustrated in appendix A. A standard data package configuration is mostly attributed to budgetary constraints and a backlog of COTS requisitioned equipment. On hand legacy equipment has been integrated with procured COTS equipment. This integration has added to the design complexity.[3]

3. Goal

To design a SNMM for the 93rd Signal Brigade data packages that describes the network management functions supporting each COTs and military device in the data packages. Also, to build upon the Open Systems Interconnection (OSI) seven-layer Management Model, the International Telecom Union-T (ITU) X.700 and X.701 System Management Model, and the International Standards Organization (ISO) Management Model demonstrating the effectiveness of such a models for instruction, and building a foundation for assessing points of integration for COTS technology into the network management operations of SOUTHCOM's Theater Network Operations Security Center (TNOSC).

4. Scope

The SNMM Model focuses on the Simple Network Management Protocol (SNMP) for network management. SNMM Model is based upon the Internet Management Model standard, and the ISO Network Management Model - concentrating on Layer

Operations,[3] Systems Management, and Layer Management. In addition, the ISO Network Management model is broke down into four models: organization, information, function and communication. In order to understand interactions between data package components and NMS workstations, our model draws upon the OSI and SNMP/Internet Models, as introduced in the future sections. The final SNMM Model does not follow the OSI or Internet Management Standards precisely, but by obeying the same rigorous principles and thought processes, the results are a model that provides a solid foundation for further study. Some basic network management concepts will be discussed.

5. Network Management Basics

Network management means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with an outdated protocol analyzer. In other cases, network management involves a distributed database, auto polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

5.1 Historical Perspective

The early 1980s saw tremendous expansion in the area of network deployment. As companies realized the cost benefits and productivity gains created by network technology, they began to add networks and expand existing networks almost as rapidly as new network technologies and products were introduced. By the mid-1980s, certain companies were experiencing growing pains from deploying many different (and sometimes incompatible) network technologies.[4]

The problems associated with network expansion affect both day-to-day network operation management and strategic network growth planning. Each new network technology requires its own set of experts. In the early 1980s, the staffing requirements alone for managing large, heterogeneous networks created a crisis for many organizations. An urgent need arose for automated network management (including what is typically called network capacity planning) integrated across diverse environments.

5.2 Network Management Architecture

Most network management architectures use the same basic structure and set of relationships. End stations (managed devices), such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing

[3] **93D Signal Brigade Field Standard Operating Procedures (FSOP).**

[4] **ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications**

one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.[5]

Management entities also can poll end stations to check the values of certain variables. Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls. Agents are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it (proactively or reactively) to management entities within NMS via a network management protocol. Well-known network management protocols include the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). Management proxies are entities that provide management information on behalf of other entities. Figure 3, depicts a typical network management architecture.[6]

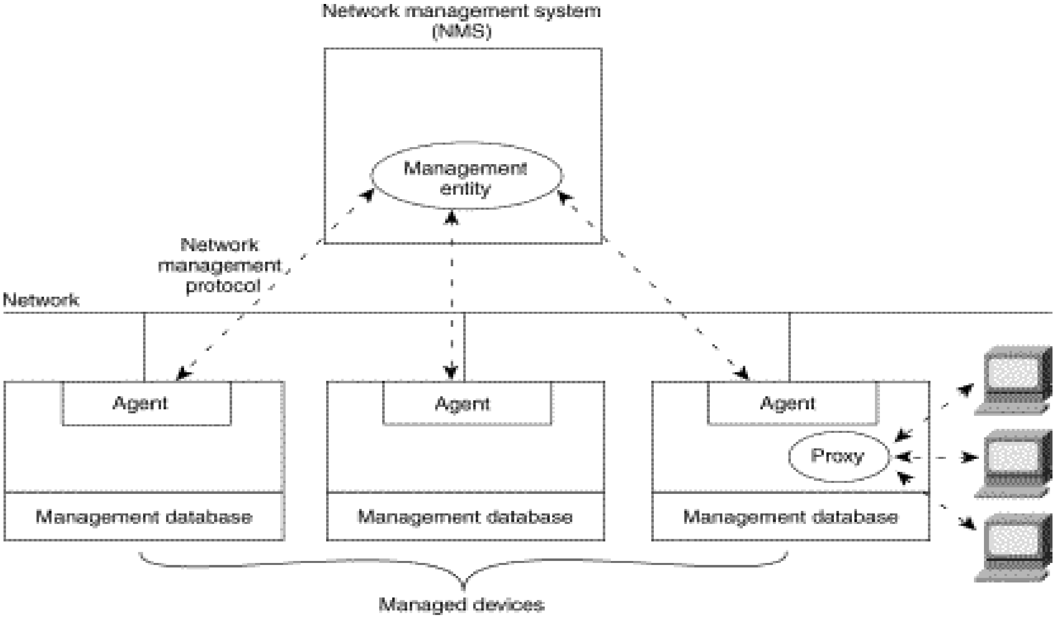


Figure 3. A Typical Network Management Architecture Maintains Many Relationships

6. Open Systems Interconnection (OSI) Management

Open System Interconnection (OSI) management standard is the standard adopted by the International Standards Organization (ISO). The OSI management protocol standard is Common Management Information Protocol (CMIP), and has built services, Common

[5] **ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications**

[6] Subramanian, Mani: “Network Management: Principles and Practice” Addisson-Wesley, New York, 2000

Management Information Service (CMIS), that specify the basic services needed to perform the various functions.[7]

OSI management discusses the possible ways to exchange management information. They are identified as systems management, layer management and layer operation. In the context of the OSI, systems management is the preferred form of management information exchange. It provides mechanisms for the exchange of information relating to the monitoring, control, and coordination of communication resources. The initial definition of systems management, as found in the OSI reference Model, distinguishes between two different properties:

1. Systems management is related to the management of OSI resources and their status across all layers of the OSI architecture.
2. Protocols for systems management reside in the application layer.

6.1 Systems Management

The first property explains what is being managed, and the second explains how management information should be exchanged. The OSI system management protocols will help project managers decide on what protocols are important at layer seven and what protocols can be used to exchange information between the manager and the agent process. In managing the data packages, the 93rd Signal Brigade uses HP Openview and What's Up Gold to manage its network status. Simple Network Management Transport Protocol (SNMPv1) is used to exchange information between the management workstation and the agent process. It is perceived that the majority of management information exchanges will require negotiation, the establishment of a management session, and a reliable end-to-end transport service. However, in our Simple Network Management Model, Figure 4, SNMP is using User Datagram Protocol (UDP), unreliable service, to transport manager to agent SNMP-PDUs.[8]

[7] Subramanian, Mani: "Network Management: Principles and Practice" Addisson-Wesley, New York, 2000

[8] ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications

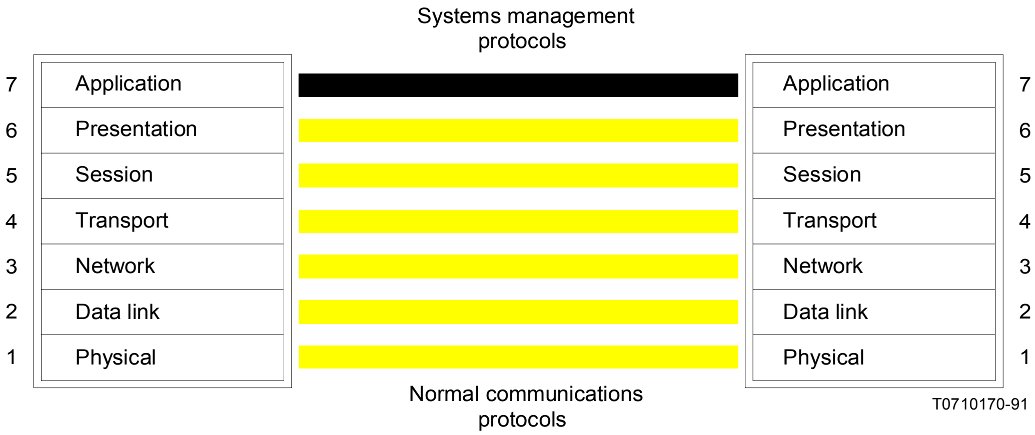


FIGURE A-1/X.700

Systems management information exchange

Figure 4. System Management

6.2 Layer Management

While systems management has been identified as the preferred method of exchanging management information, layered management is used in special circumstances to carry information specifically to the operation of an N-layer. At layer management, User Datagram Protocol (UDP) is used to deliver SNMP-PDUs end-to-end. Protocol analyzers or access list can be used to manage packets, i.e. traffic shape, going across the network. Also, for example, layer management is commonly used for the exchange of routing information. In a number of cases, routing information must be broadcasted over an entire routing domain. Since the presentation service has no broadcast capabilities, it may be inefficient to use systems management. See Figure 4.1.[9]

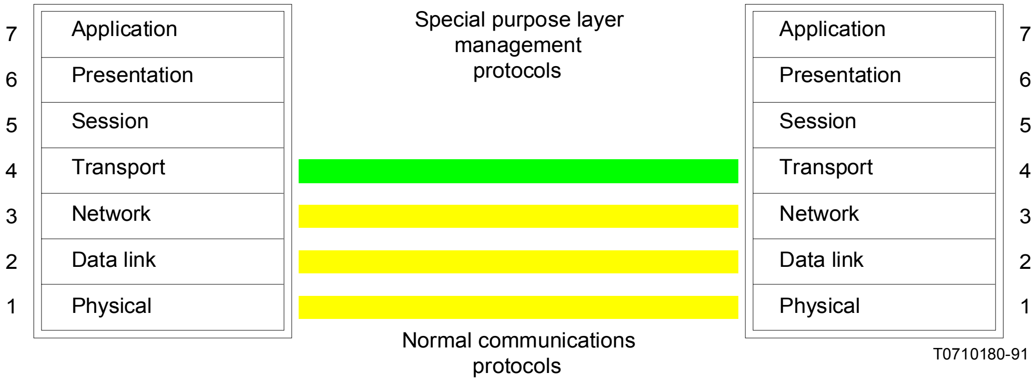


FIGURE A-2/X.700

(N)-Layer management exchange

Figure 4.1. Layer Management

[9] ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications

6.3 Layer Operations

The last type of management information exchange is layer operation. It is defined in the standard as the set of facilities that control and manage a single instance of communication. At layer 3, access list, sniffers, and firewalls are used to manage IP networks. At layer 2, data link layer, SNMP traps can be setup to alert network managers that links are down or in error. Meter Reports from the switch databases are used at this layer to manage link status and performance. Last, at layer 1, data package operators to manage and control status of layer 1 errors use Firebirds and flute line testers, See Figure 4.2.[10]

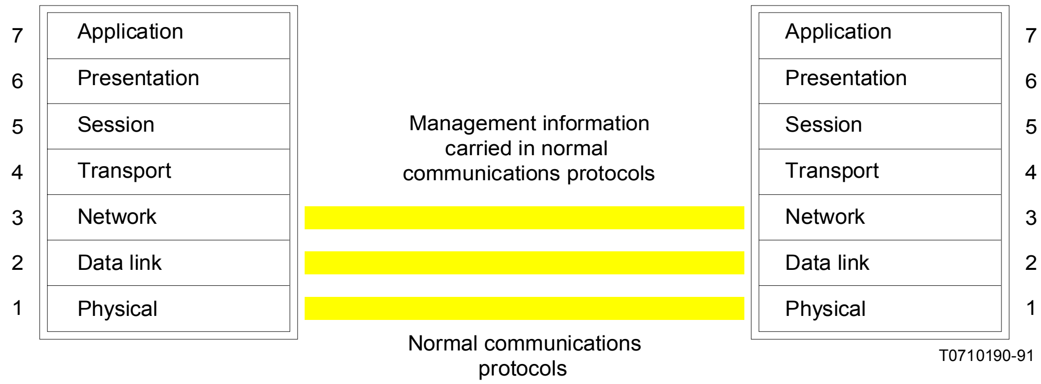


FIGURE A-3/X.700

(N)-layer operation

Figure 4.2. Layer Operations

6.4 Summary

The OSI model was used to evaluate the 93rd Signal Brigade's Data packages, but what we found through research is that the data package devices overwhelming have SNMPv1 resident in their operating systems or firmware. Thus, this will allow us to define a suggested model that will better explain how the 93rd Signal Brigade can manage their data package.

OSI Layers	Purpose	Management Tool
Applications	Systems Management	HPOpenView; CSCE; Whats Up Gold
Presentation	CMIP; SNMP; Encryption	KIV-19; KIV-7HS
Session	CMIP; SNMP	MIB Browsers
Transport	TCP; UDP	Protocol Analyzers

[10] ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications

Network	IP	Access list; Firewalls; Sniffers, ICMP msgs
Data Link	HDLC/PPP	Metering Reports ; Systems Integrator
Physical	802.3	Firebirds; Flutes

Figure 4.4. Summary of OSI Network Management

7. ISO Network Management Model

The ISO Network Management Model is broken down into four different models. The models explain how Network Management Systems communication to agents resident in network devices.

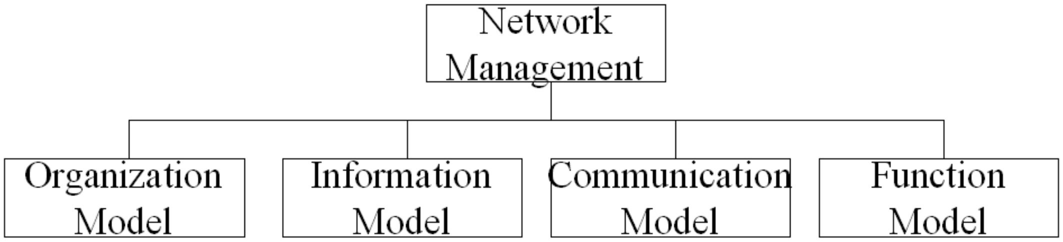


Figure 5. Summary of OSI Network Management[11]

7.1 Organization Model

Components of the data communications package can be classified into managed or unmanaged objects or elements. The managed elements have a management process running on them called agents. The manager communicates with the agent in the managed element. The manager queries the agent and receives management data, process it, and stores the results in its database. The agent may also send a minimal set of information to the manager unsolicited.

[11] Subramanian, Mani: “Network Management: Principles and Practice” Addisson-Wesley, New York, 2000.

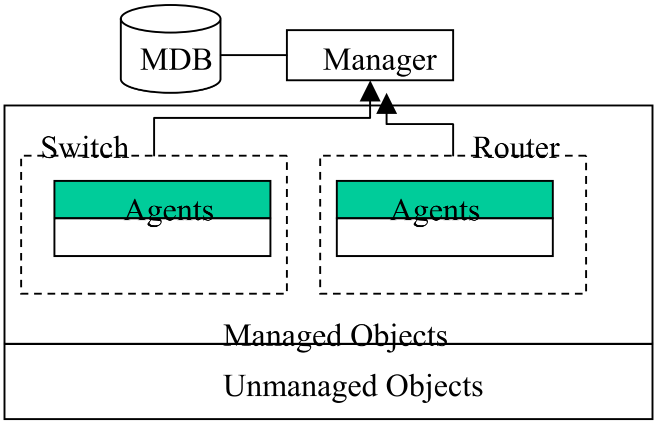


Figure 5.1. Network Management Framework

7.2 Information Model

The information model specifies the information base to describe managed elements and their relationships. The Structure of Management Information (SMI) defines the syntax and semantics of management information stored in the Management information Base (MIB).[12]

Management information bases (MIB) are a collection of definitions, which define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each of the definitions written in the MIB. It is not the actual database itself - it is implementation dependant. Definition of the MIB conforms to the SMI given in RFC 1155. Latest Internet MIB is given in RFC 1213 sometimes called the MIB-II. You can think of a MIB as an information repository.

[12] Subramanian, Mani: “Network Management: Principles and Practice” Addisson-Wesley, New York, 2000.

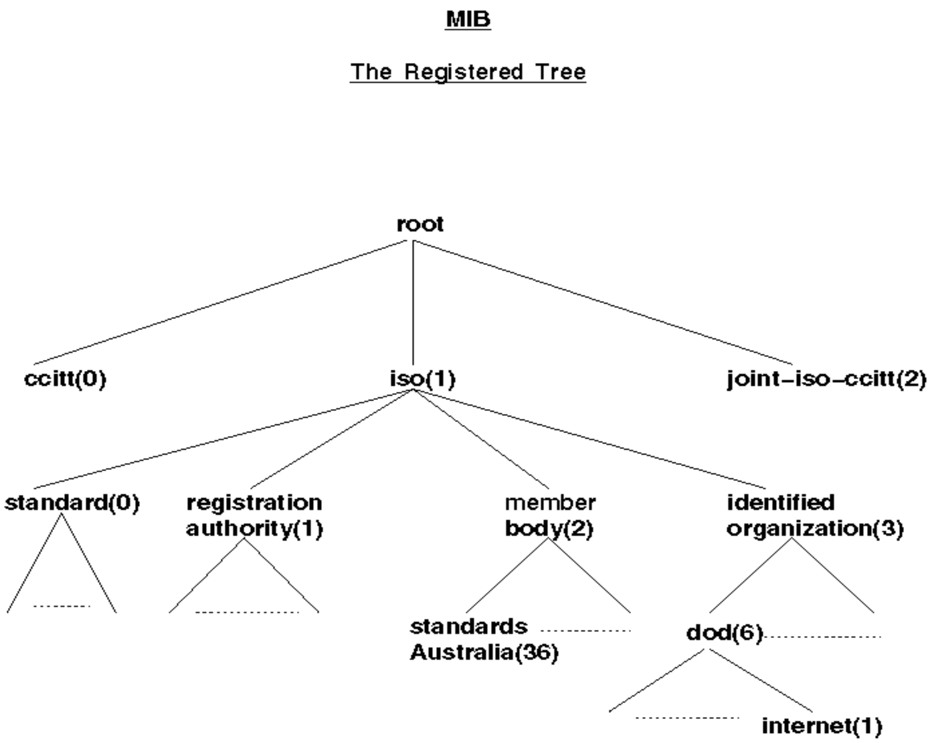


Figure 5.2. Register MIB Tree[13]

If agent is to be SNMP manageable then it is mandatory to implement the Internet MIB (currently given as MIB-II, RFC 1157). The Management Information Trees (MIT) defines a tree structure that defines managed objects. During our research, we were able to verify that the network management software they were using actually did go out and pick up MIBs from specific IP addresses, which proved our model. By looking at the following example, you can see how What's Up Gold sent out a GET-request and received an SNMP-Response PDU back with the appropriate MIB object. The 1.3.6.1.1.576.19.1.2.1.1.1.1.18.9 is a General Dynamics MIB (**576**) object identifier.

7.3 Communications Model

The communications model component of the OSI addresses the way information is exchanged between systems. Management data is communicated between agent and manager processes, as well as between manager processes, as represented with the data packages. There are three aspects of communications between two entities: transport medium of message exchange; message format of communications; actual responses. The Internet uses SNMP for communications. The services are part of operations using requests, responses, and alarms notifications. The Internet uses connectionless UDP/IP protocol to transport messages. The communication management of the data packages over the WAN occurs utilizing the following process. With HP Openview, managers can communicate with agent that is loaded on SNMP enable devices.

[13] ITU-T: X. 701 Information Technology - Open Systems Interconnection - Systems Management Overview.

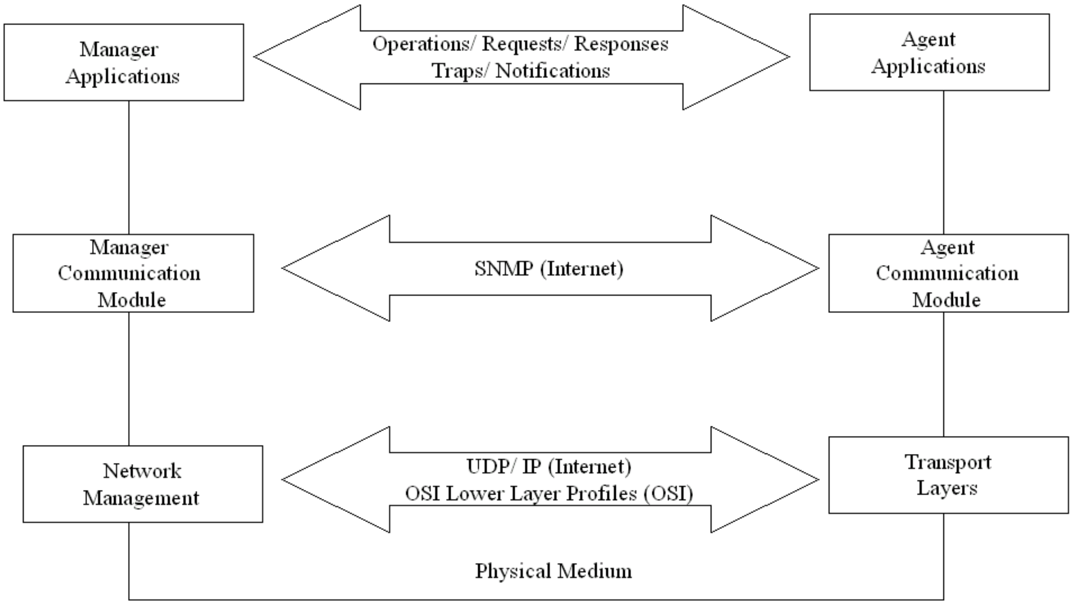


Figure 5.3. Management Communication Transfer Protocols[14]

7.4 Functional Model

The functional model component of the OSI addresses the user-oriented applications. The functional models consist of five sub models: fault management, accounting management, configuration management, performance management, and security management.

7.4.1 Fault Management

Fault management enables detection, isolation and correction of abnormal operations. Abnormal operations may be caused by design and implementation errors, overload errors, or external disturbances. Fault management includes functions to:

1. Maintain and examine error logs
2. Accept and act upon error notifications
3. Trace and identify faults
4. Carry out diagnostic test
5. Correct faults.

Fault in a network is normally associated with the failure of a network component and subsequent loss of connectivity. Fault Management involves a five-step process: (1) fault detection, (2) fault location, (3) service restoration, (4) identification of the problem's root cause, and (5) problem resolution. Fault should be detected as quickly as possible by

[14] Subramanian, Mani: "Network Management: Principles and Practice" Addisson-Wesley, New York, 2000.

the centralized management system. The 93rd Signal Brigade's TNOSC utilizes HP Openview as its centralized management system. HP Openview manages switched layer 2 and routed layer 3 environments, i.e. devices; shows a filtered view of the managed network; provides views of protocols running on the network; launches targeted views from events for rapid problem resolution. The Remedy Trouble Ticketing System is also a tool that the TNOSC has incorporated into its automated network operations system for problem resolution. However, this tool is dependent on user input into separate reporting system, thus not real-time.

Fault location and isolation techniques are not encompassed in one vendor software or management system for data packages. The 93rd Signal Brigade utilizes various tools and network devices to isolate network components that have failed that are not layer 2 or layer 3 devices. Layer 1 devices, such as KIV-19s, KIV-7s, KG-194s, pairgain modems, and CV-2048s, have fault alarms that are currently not being remotely monitored by the TNOSC. The equipment maintainer is performing fault management.

The 93rd Signal Brigade, the TNOSC and the subordinate SYSCONs currently are able to perform Layer 2 and layer 3 fault management on routers, switches, FCC-100s, Network Encryption System (NES), workstations, servers, etc. Various diagnostic tools to isolate the cause are doing this: What's Up Goal; HP Openview; Communications System Control Element (CSCE). These tools determine failure of the component or failure of the physical link or interface by pinging. Excessive pinging by multiple network management tools causes network degradation and potential outages. Bandwidth efficiency is impacted at the expense of fault management.

The Simple Network Management Model can improve upon the 93rd Signal Brigade's fault management and detection. By enabling SNMP on data package component and network devices, proactive polling, traps and agents can be installed with minimal degradation or impact to the network.

7.4.2 Accounting Management

Accounting Management enables charges to be established and cost to be identified for the use of network resources.

Accounting management includes:

- Inform users of the cost
- Inform users of the expected costs in the future
- Set cost limits

Accounting Management is associated with corporate and/or nonmilitary organizations that are normally operating in revenue driven environment. 93rd Signal Brigade does not currently utilize any accounting management tools or services to monitor, control or interconnect activities in support of the data packages.

7.4.3 Configuration Management

Configuration management identifies, exercises control over, collects data from and provides data to open systems for the purpose of preparing for, initializing, starting, providing for the continuous operation of, and terminating interconnection services. Configuration management includes:

- Records changes in the configuration
- Records the current configuration
- Identifies network components (give addresses to Service Access Points and titles to Network entities)
- Initiates and closes down managed objects
- Changes network parameters i.e. routing tables.
- Collect information on demand about the current condition of the open system

The 93rd Signal Brigade, the TNOSC and its subordinate SYSCONS are capable of displaying static or permanent configurations of the network and the data packages. The status of the network is displayed by network management systems. However, the brigade is unable to display dynamic configuration of network component failures, as well as traffic patterns and performance.. The TNOSC and the subordinate SYSCONS utilize HP Openview, the CSCE Workstations and What's Up Gold for static configuration management. Also, the brigade manages the configuration of routers by telnetting into Cisco routers.

The team submits that the 93rd Signal Brigade can address dynamically changes to the configurations of networks and their components with the purposed SNMM. Relevant SNMP management information is embedded in managed objects such as switches, hubs, bridges, routers, NESs, AN/FCC-100, the Single Shelter Switch (SSS) Console Workstation Configuration management involves setting up parameters. For example, alarm thresholds could be set to generate alarms when packet loss exceeds a defined value. Information on the object name and the person to be contacted when the component fails could be entered into management agent. The configuration data is gathered automatically by and stored in the NMS at the TNOSC, which is displayed real time.

7.4.4 **Performance Management**

Performance management is needed to optimize quality of service. To detect changes in the network's performance, statistical data should be collected and logged on an incidental or periodical basis. Logs are not restricted to the use of performance management they may also be used by:

- Gather statistical information
- Maintain and examine logs of system histories
- Determine system performance under natural and artificial conditions

- Alter system modes of operation for the intent of conducting performance management activities

The 93rd Signal Brigade has at its disposal various tools for performance management. They are the CSCE, HP Openview and What's Up Gold. By enabling embedded SNMP agents on network and data package devices, network statistics can be captured on traffic volume, availability, management and delay. Performance data on availability and delay is useful for tuning the network to increase its reliability and to improve its response time. In order manage performance, data must be gathered by the TNOSC and kept up to date. If changes are required, they can be administered by the TNOSC. The SNMM allows you to analyse the various application-oriented traffic such as web traffic, Internet mail, file transfers, etc. SNMP enabled devices can be evaluated capturing statistical trends utilizing tools such as, What's Up Gold, CSCE and HP Openview. These statistics can therefore be used to make policy decisions that affect the management of the network.

7.4.5 Security Management

Security management is the set of facilities that enables the manager to initialize and modify those functions that secure the network from user misbehavior and unauthorized access. Importances of security management are key management, maintenance of firewalls, and creation of security logs.

- The creation, deletion and control of security services and mechanisms
- The distribution of security relevant information
- The reporting of security relevant events

Security management covers a broad range of security aspects. Physically securing the network, access to the network resources, and secured communications over the network. Military communications operate in secret high networks. Transmissions paths are bulked encryption. Network devices and protocols at nearly each layer of the OSI Model encrypt traffic. The 93rd Signal Brigade utilizes Firewalls, Intrusions Detections Systems (IDS) Monitors, Router Access Control Lists (ACL), Signal Encryption Devices, NES, and Server software to maintain network security. Routers, Intrusion Detection Systems, Servers, and Network Encryption Systems contain SNMP protocols that support security management. Security parameters such as polling, traps and alarms can be configured to determine intrusions, events and incidents. Unauthorized access generates an alarm to the NMS at the TNOSC. The 93rd currently has HP Openview as their NMS, which SNMP is enabled. The SNMM supports security management.

8. Design Model

A good network management design can help an organization achieve availability, performance and security goals. Effective network management processes can help an organization measure how well design goals are being met and adjust network parameters if they are not being met. Network design should be approached the same way design projects are approached.[15] Think about scalability, data formats, and cost/benefit tradeoffs. Network management systems can have a negative effect on network performance. The amount of polling can be significant enough to cause network failures. But, with the use of RMON and SNMP Traps, network operators will use a small portion of the bandwidth.

Network management architecture consists of managed devices, agents, and NMS arranged in a topology that fits into the internetwork topology, See figure 6. The task for designing a network management model parallels the tasks for designing an internetwork. Traffic flow and load between NMS and managed devices should be considered. Other design considerations are whether or not traffic flows are in-band or out-band. A decision should be made regarding a centralized or distributed management topology.

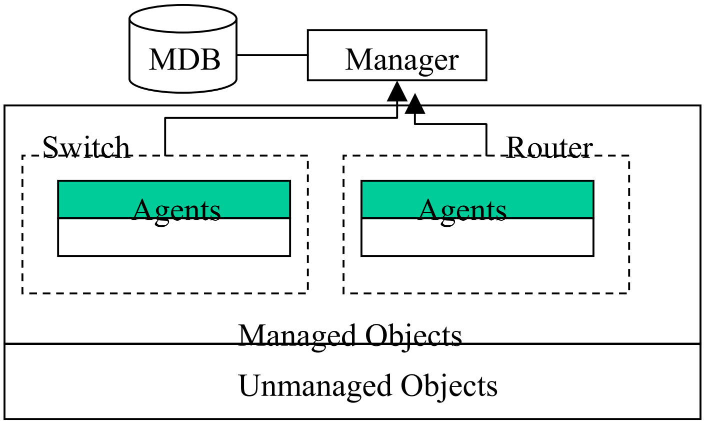


Figure 6. Manager-Agents Relationship[16]

8.1 Design Goals

The design goal of the team was to build a Simple Network Management Model that will assist the 93rd Signal Brigade with the management of their deployable data packages. Five parameters were used to determine what our model would look like: bandwidth usage, proactive network management, SNMP enabled, simplicity, central management and cost. During the research of each device, researches found that the SNMPv1 was resident in most devices in the data package. SNMPv1 is truly simple, as its name indicates. Also, known as the Internet Model, the SNMP/Internet model is easy to implement, and widely used (see figure below) between commercial and DOD vendors. Because the Army uses a lot of legacy equipment, SNMPv1 was researched to be the easiest to implement and cheaper to upgrade.

[15] Oppenheimer, Priscilla, Top-Down Network Design, 1999, Macmillan Technical Publishing.

[16] Subramanian, Mani: "Network Management: Principles and Practice" Addisson-Wesley, New York, 2000.

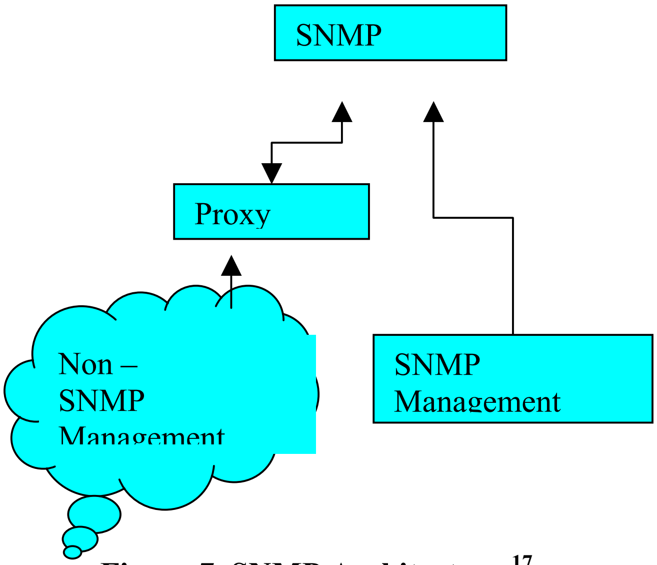


Figure 7. SNMP Architecture [17]

One of our design objectives is to ensure that all of the SNMP enabled and non-SNMP devices within the data packages can be remotely managed. The 93rd Signal Brigade uses HP Openview, What's Up Gold, Systems Integrator, and CSCE as their Network Management Systems Tools. These tools can employ intermittent polling (ICMP Pinging) of network agents within the network devices to update their topological diagrams in near real time. The pinging uses up a lot of bandwidth but with RMON and SNMP traps bandwidth usage can be minimized. So, pinging will be held to a minimum and other methods of using SNMP will be suggested. Based on research most of the devices in the data package can be SNMP enabled and are RMON capable.

In system management, HP Openview, What's Up Gold, ISYSCON are used at the application layer. In layer operations, the bottom three layers of the OSI model, the 93rd Signal will use a FIREBIRD at the physical and data link layers; FLUTE line testers at physical layer, and Packet Sniffers Ethereal and etc. at the network layer. SNMP-based network management is widely used for campus wide network SNMPv1 will be the best choice in managing tactical networks. In addition, the following are the design goals defined:

1. **Bandwidth usage**: In the tactical environment, bandwidth is a limited resource. Because equipment constraints and terrain, tactical communication systems designs, signal units are limited on the amount of bandwidth that they can provide. The network management system that is provided has to be able to work

[17] Subramanian, Mani: "Network Management: Principles and Practice" Addisson-Wesley, New York, 2000.

in this band-limited environment. Bandwidth is measured in bit per second and by the percentage of data traffic it utilizes.

2. **Proactive Network Management**: Network Management should be proactive. Proactive management means checking the health of the network during the normal operations in order to recognize potential problems, optimize performance and plan upgrades. Being proactive means that Network Operation Centers (NOC) must collect statistics and conduct tests, such as response time measurements, on a routine basis. The statistics and test results can be used to communicate trends and network health to management and users. In our design, SNMP allows network managers to set traps in certain places within the network to collect specific traffic data, or use RMON to automatically collect traffic data.

3. **SNMP and non-SNMP enabled managed device:** It is important that the devices in the data packages have a common version of SNMP. Now, there are other transport protocols that can be used to management networks, Common Management Information Protocol (CMIP), LAN Network Manager (LNM), ICMP pings, and etc. But, our team has decided to use SNMP to managed 93rd Signal Brigade's packages. The fact is that the Army uses legacy equipment that came with SNMPv1 resident within its firmware or operating system, like AN/FCC-100 (V)7. So, SNMP was common to most if not all of the devices that can be managed.

DEVICES	PURPOSE	SNMP ENABLED (Y/N)	NETWORK MGT SYSTEM	VENDOR
FCC-100 (V) 7	MUX	Y	WHATS UP GOLD	DNE
PAIRGAIN	LINE DRIVER	Y	WHATS UP GOLD	LTI DATACOMM
CISCO 3640	ROUTER	Y	WHATS UP GOLD	CISCO
CATAYIST 2950	SWITCH	Y	WHATS UP GOLD	CISCO
SNAP SERVER	FILE SEVER	Y	WHATS UP GOLD	IGOV
DOMAIN CONTROLLER	PDC SERVER	Y	WHATS UP GOLD	COMPAQ
KIV-7HDS	ENCRYPTION	N	NONE	TITAN
KIV-19	ENCRYPTION	N	NONE	TITAN
CV-2048 CODEM	LINE CONVERSION	Y	WHATS UP GOLD	DNE
KG-194	ENCRYPTION	N	NONE	TITAN

4. **Centralized Management:** The TNOSC is the central place where the 93D Signal Brigade wants to manage its data packages, as they are forwardly deployed. Central management involves one area where the network management workstation or process is located. During deployments the TNOSC will be able to remotely monitor data packages for faults, performance, accountability, configuration and security.

5. **Simplicity:** Webster's dictionary defines simple as having only one thing, element or part. In our definition widely used and already available - meaning the same protocol resident on all devices, helps define what we mean by simplicity.

6. **Cost:** the amount of funding expense that will be used to develop a NMS to manage the data packages from the TNOSC.

8.2 The Simple Network Management Model (SNMM)

SNMM is a simple model that allows users and students to understand how network management can happen in tactical environments. The model is based on SNMP/ Internet and OSI model concepts. The figure illustrates how a network management system queries an agent process for status. SNMP is the transport protocol used in our model to talk from the manager to the agent.

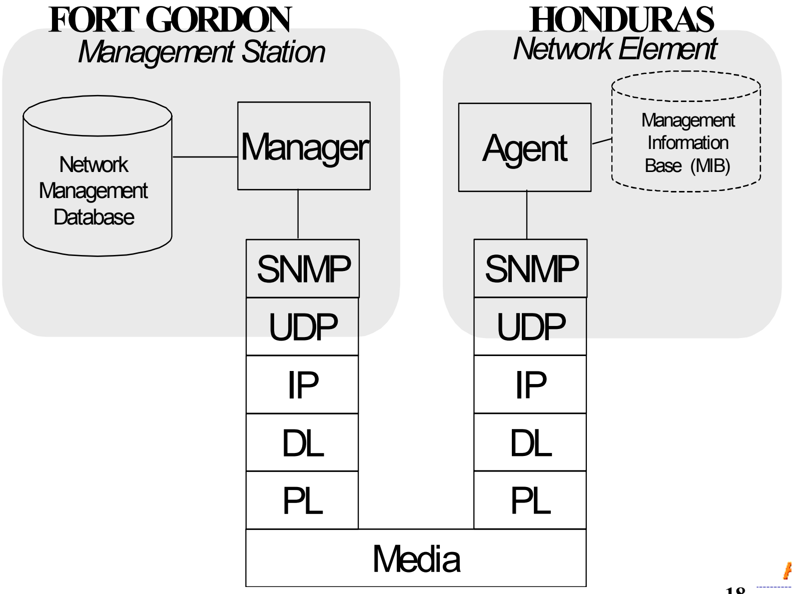


Figure 8. Simple Network Management Model[18]

The model is simple because it uses protocols that are common in legacy and future devices. SNMP is the transport protocol of choice in the SNMM that is used to send and receive request to or from network elements like routers and managed hubs. Our model demonstrates how management of the data packages from remote sites can be accomplished.

[18] Network Management, Telecom Systems Engineer Course, FA24 Lecture Notes.

9. Data Collection and Analysis

In order to validate the SNMM model, the authors used a specific management tool set to verify that SNMP queries were sent to each device. So, first, the authors selected tools that were common to 93rd Signal Brigade and the research team. Next, the authors use three phases to validate that SNMP traffic was alive on the network.

9.1 Tool Selection

There are several tools available on the commercial market for use in the managing networks. In the SNMM model, researchers used What's Up Gold to monitor, analyze and manage the network. What's Up Gold resides at layer 7 (Application Layer of the OSI Model). The program utilizes SNMP queries to retrieve information about the network. Management tools that utilize SNMP use get, set and get-next messages to extract response messages from agents (which get the information from the objects located on the physical devices) to paint a picture of the status of the equipment attached to the network devices.

Utilizing protocol analyzers (more commonly called sniffers), researchers were able to validate that the SNMP messages flow through the network from managed devices to network management software workstations. The SNMP messages are encapsulated into UDP-PDU at the Transport Layer, which is further encapsulated into IP-PDU at the Network Layer. It is then further encapsulated into Ethernet, which is transferred to its intended device via Cat 5 cable, 802.3. The screen capture in Appendix XX demonstrates how using Ethereal Protocol analyzer program captures "get-next" request and agent response packets.

9.2 Data Collection

The data collection and analysis phase of this research project was conducted in three phases:

- Phase I - Product research
- Phase II - Lab testing
- Phase III - Field testing

During the product research phase researchers gathered information from the 93rd Signal Brigade concerning what applications they currently use to perform network management. Also, they searched the Internet and trade journals for other management applications to develop a tool set. After compiling this information researchers decided to use HP OpenView and What's Up Gold for the network management system (NMS). The authors decided to use these management applications because they wanted to develop a management model that would actually be feasible for the 93rd Signal Brigade. These two applications were easy to use and free firmware on the Internet. Some of the other applications were cost prohibitive and required more training. When selecting a data capture application researcher chose Ethereal because of its ease to use and price. Some other applications could do the same job, however, they were cost prohibitive. When selecting a trace program, researchers chose NeoTrace because of its ease to use and graphical user interface. NeoTrace allowed researchers to attain a graphical traceroute of IP addresses that made it easy for the team to identify where gateway routers and servers were located. It also gave the team statistics such as ping response times and provided color codes for the status of the links.

During the lab testing, researchers connected two data packages together and simulated a link between two networks. Researches validated that they had connectivity from one data package router to the other distant end routers and PCs. The team confirmed that they could actually communicate with the distant end by receiving IMCP Pings back from Cisco routers and other networked devices at the far end. The lab results confirmed that the field test architecture would work. Also, the lab test proved that an IP scheme needed to be preplanned and SNMP agents on data package devices should be enabled at the command prompt of data package devices.

During the field-testing phase of the research project, the team validated that the SNMP management information was being passed on the network. This was accomplished by forcing "get" requests in the network at specific time so that the team could capture and analyze the packets. From doing this several times, researchers were able to capture several "get requests" and responses from server, router and other managed devices. Because researchers wanted to keep their packet captures to a reasonable size, the packet capture that was cut off and lasted about 60 seconds to capture 1000-1200 packets. Most of the packets captures were TCP.

By using the packet capture utility, researchers were able to verify that the network management software they were used actually did request out and retrieve MIBs object ids from specific devices with IP addresses, which proved our model. By looking at the following example, you can see how WhatsUp Gold sent out a GET-Request and received an SNMP-Response PDU back with the appropriate MIB object. The 1.3.6.1.1.576.19.1.2.1.1.1.1.18.9 is a General Dynamics MIB (**576**) object identifier.

The screen shot, in appendix C, displays the statistical analysis of one of the data captures. The area that the team was concerned with is the number and percentage of SNMP packets that go through the system. As you can see, approximately 15% of the packets were SNMP (15% of the traffic flow was used for this). This validates that the SNMM model is working between manager and agent processes.

10. Conclusion

The SNMM Network Management Model provided in this paper is by no means complete. Just as volumes have been written to describe what happens at each of the layers of the OSI model, one would expect that the SNMM Model would similarly result in more detailed documents explaining specific aspects of key protocols and layers. For instance, some resident agent on the devices must manage the KIV-19 and 7HS used in the data packages. Trying to acquire that kind of information is difficult because of the security classifications of the devices. The possible development of MIBs to manage end-user devices are all worthy of additional investigation. The importance of the simple management model presented in this paper is that it establishes the solid framework required for precisely this kind of study, development, and application.

10.1 Network Management of future communications networks

The SNMM Model certainly does provide some key insights into how COTs and military devices can be managed in the future. This relationship between military and commercial off-the-self equipment is the future of military communications networks. By managing network devices, the authors can provide better security, quality service, and performance management.

The network management model framework provides a reference for future study. The OSI management model is an excellent way of providing analysis on how management is occurring at different layers of the OSI model. But, the OSI is a reference only; it falls short in explaining how network management is really happening in real-time. SNMN model better explains how the 93rd Signal Brigade is really going to manage the data packages. The OSI standard uses the CMIP protocol to talk from manager workstation to agent process. CMIP is not used in any device in the data packages.

In the future network will become more complex. The ability to manage these networks will be the key to the future of Signal Operations.

10.2 Recommendations

The following are recommendations to the 93rd Signal Brigade on how to manage their data packages: develop a common set of management tools, enable all SNMPv1 agents on data package devices and manage non-SNMP devices by using a REMEDY trouble ticket system.

10.3 Conclusions

The usefulness of the SNMM model in evaluating unique requirements for military communications systems is indicative of its usefulness as an Army Signal Corps standard. In researching the paper, the authors discovered that the ability to describe network management system processes in terms of the OSI and Internet models gave them credibility, a common ground for discussing complex ideas, and a framework for explaining the interrelated ideas of user, performance, security, and management. Obviously, the laws of physics have not changed, and the techniques used in developing SNMM are just as valid whether they are presented in accordance with a layered protocol or reference model. Nevertheless, the time has come to evaluate all communications systems from a model prospective. Army signal personnel should learn about network management in terms of common models. Their ability to understand systems in terms of industry models will help them to take advantage of the convergence of military and commercial technologies, understand legacy systems and identify strategies for upgrading or replacing them, and, perhaps most importantly, teach them the language of telecommunications.

The SNMM Model demonstrates the effectiveness of applying current industry telecommunications models to understand legacy communications systems. These models provided a framework for identifying key pieces of the system's architecture, and established a foundation for further study. The model helped to identify strengths and weaknesses of the existing data communications system, and suggested logical points to insert new technology. Finally, it demonstrated that the use of familiar models makes it possible to learn about any unfamiliar system very quickly. Technology changes more rapidly each year, but simple models allow telecommunications engineers, professionals, and end users to efficiently assess key features, capabilities, and weaknesses. These models are invaluable in keeping up with legacy, current, and future communications systems.

CITATIONS

1. Smith, Marina,:"Virtual LANS", McGraw Hill, New York, 1998

2. Subramanian, Mani: "Network Management: Principles and Practice" Addisson-Wesley, New York, 2000

3. Oppenheimer, Priscilla : "Top-Down Network Design", Macmillan Technical Publishing, Indianapolis, 1999

4. Sheldon, Tom: "Encyclopedia of Networking and Telecommunications", McGraw-Hill, page 1159, New York, 2001

5. Case, J., Fedor, M., Schoffstall, M. and J. Davin, "Simple Network Management Protocol", STD 15, RFC 1157, May 1990

6. McCloghrie K., and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets", RFC 1156, Hughes LAN Systems, Performance Systems International, May 1990.

7. ITU-T: X .700 Management Frameworks for Open Systems Interconnection (OSI) for CCITT Applications

8. ITU-T: X. 701 Information Technology - Open Systems Interconnection - Systems Management Overview

9. Field Manual (FM) 6-02.71 (11-71), Network Management (NM), Draft, July 2000

10. Network Management, Telecom Systems Engineer Course, FA24 Lecture Notes

11. 93D Signal Brigade Field Standard Operating Procedures (FSOP)

Appendix A - Data Package Components

Box	Equipment	Purpose
NIPR	Cisco 3640 Router/ Firewall	IP Routing/ Security
	Cisco 2920 Switch	User Network Access
	NES	Data Encryption
	Server	PDC, IDS
	Server	BDC, IDS, Ghost, IIS
	Server	Exchange
	SNAP Fileserver	Network Access
	Pairgain Modems	Signal Line Driver
	Monitor	Intrusion Detection System
	UPS	Uninterupted Power Supply
SIPR	Cisco 3640 Router/ Firewall	IP Routing
	Cisco 2920 Switch	User Network Access
	Server	PDC, IDS
	Server	BDC, IDS, Ghost, IIS
	Server	Exchange
	SNAP Fileserver	Network Access
	Pairgain Modems	Signal Line Driver
	KIV-7	Signal Encryption
	Monitor	Intrusion Detection System
	UPS	Uninterupted Power Supply
Transmission	FCC-100	Level 1 Multiplexer
	KIV-19 or KG-194	Signal Encryption
	CV-2048	Signal Conversion
VTC	POLYCOM Base Unit w/ Flat Screen Monitor	Point-to-Point Video Teleconference

Appendix B - Simple Network Management Protocol

Introduction

Since its initial development in 1988, Simple Network Management Protocol has become the standard for internetwork management. Vendors can easily implement SNMP into their products because it requires little code to implement. Because SNMP is extensible, it allows vendors to easily add network management functions to their existing products. SNMP additionally separates the management architecture from the architecture of the hardware devices, which expands the base of multivendor support. Unlike other network management protocols, SNMP is an implementation that is widely available today.

SNMP is based on the manager/agent model. SNMP is referred to as "simple" because the agent requires minimal software. Most of the processing power and the data storage is located on the management system, while a complementary subset of those functions resides in the managed system. To achieve its goal of being simple, SNMP includes a limited set of management commands and responses. The management system issues Get, GetNext and Set messages to retrieve single or multiple object variables or to establish the value of a single variable. The managed agent sends a Response message to complete the Get, GetNext or Set. The managed agent sends an event notification, called a *trap* to the management system to identify the occurrence of conditions such as threshold that exceeds a predetermined value. In short there are only five primitive operations:

- get (retrieve operation)
- get next (traversal operation)
- get response (indicative operation)
- set (alter operation)
- trap (asynchronous trap operation)

- **Get Request.** Specific values can be fetched via the "get" request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device.

- **Get Next Request.** The SNMP standard network managers to "walk" through all SNMP values of a device (via the "get-next" request) to determine all names and values that an operant device supports. This is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a "get-next", and repeating this operation until an error is encountered (indicating that all MIB object names have been "walked".)

- **Set Request.** The SNMP standard provides a method of effecting an action associated with a device (via the "set" request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. This provides a way of configuring and controlling network devices via SNMP.

- **Trap Message**. The SNMP standard furnishes a mechanism by which devices can "reach out" to a network manager on their own (via the "trap" message) to notify the manager of a problem with the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

7.2 SNMP Message Construct

Each SNMP message has the same format consisting of the version number, community name (similar to a password), and one or more SNMP-PDUs (assuming trivial authentication). Every SNMP PDU (except trap) consists of the following format:

- Request id - request sequence number
- Error status - zero if no error otherwise one of a small set
- Error index - if non zero indicates which of the OIDs in the PDU caused the error2
- List of OIDs and values - values are null for get and get next

Trap PDUs have the following format:

- Enterprise - identifies the type of object causing the trap
- Agent address - IP address of agent which sent the trap
- Generic trap id - the common standard traps
- Specific trap id - proprietary or enterprise trap
- Time stamp - when trap occurred in time ticks
- List of OIDs and values - OIDs that may be relevant to send to the NMS

7.3 What does SNMP access?

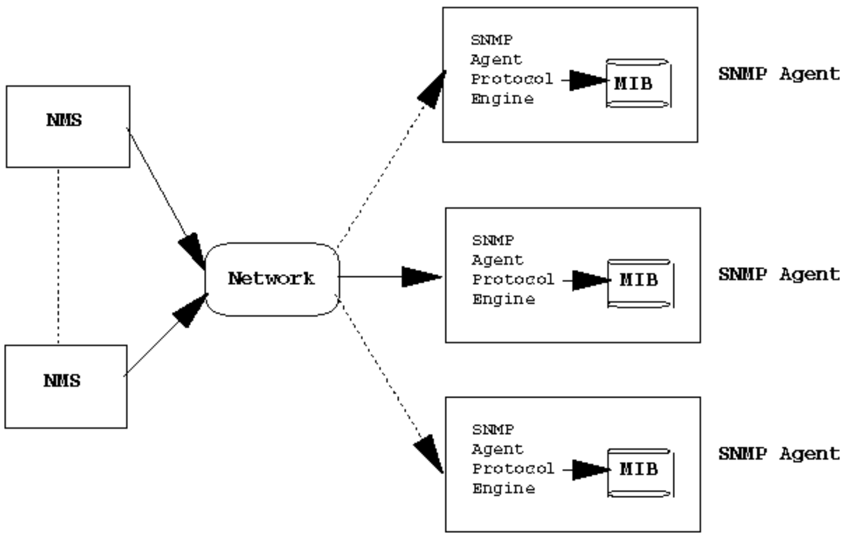
SNMP accesses particular instances of an object. All instances of an object in the MIB reside at the leaf nodes of the MIB tree. SNMP Protocol accesses objects by forming an Object identifier of form x.y where x is the "true" OID for the object in the MIB, and y is a suffix specified by the protocol that uniquely identifies a particular instance (e.g.. when accessing a table).

- For primitive single instance leaf objects use y=0
  for example: sysDescr (OID: 1.3.6.1.2.1.1.1) would be referenced in the SNMP protocol by 1.3.6.1.2.1.1.1.0 (i.e. sysDescr.0)
- For single instance of columnar leaf objects (i.e. one instance from a table type of object) use y=I1.I2.I3

7.4 Network Management Architectures

Network management system contains two primary elements: a manager and agents. The Manager is the console through which the network administrator performs network management functions. Agents are the entities that interface to the actual device being managed. Bridges, Hubs, Routers or network servers are examples of managed devices that contain managed objects. These managed objects might be hardware, configuration parameters, performance statistics, and so on, that directly relate to the current operation of the device in question. These objects are arranged in what is known as a virtual information database, called a management information base (MIB). SNMP allows managers and agents to communicate for the purpose of accessing these objects. The model of network management architecture looks like this:

Architecture


NMS
NMS
Network
SNMP Agent Protocol Engine
MIB
SNMP Agent
SNMP Agent Protocol Engine
MIB
SNMP Agent
SNMP Agent Protocol Engine
MIB
SNMP Agent

A typical agent usually:

- Implements full SNMP protocol.
- Stores and retrieves management data as defined by the Management Information Base
- Can asynchronously signal an event to the manager
- Can be a proxy for some non-SNMP manageable network node.

A typical manager usually:

- Implemented as a Network Management Station (the NMS)

- Implements full SNMP Protocol
- Able to
    - Query agents
    - Get responses from agents
    - Set variables in agents
    - Acknowledge asynchronous events from agents

Some prominent vendors offer network management platforms that implement the role of the manager (listed in alphabetic order):

- Dec PolyCenter Network Manager
- Hewlett-Packard OpenView
- IBM AIX NetView/6000
- SunConnect SunNet Manager

MIB traversal using GetNext operation

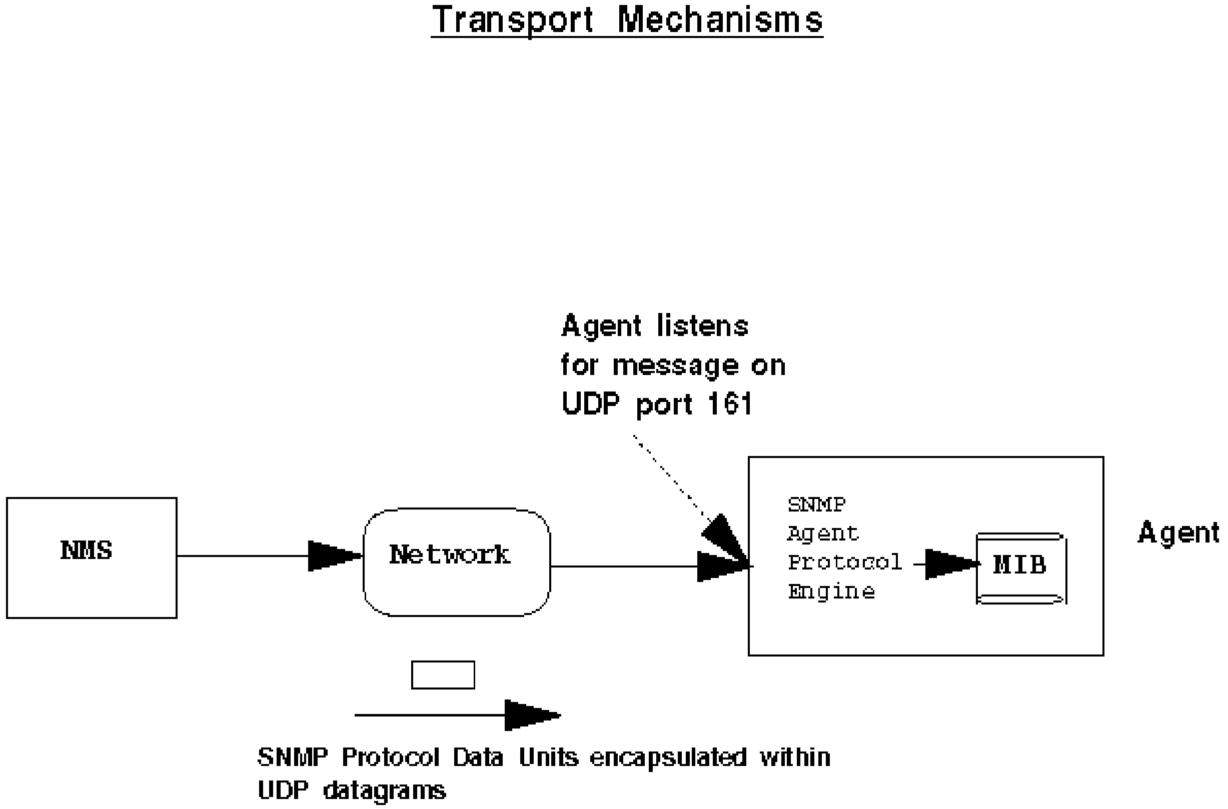
Underlying communication protocols

SNMP assumes that the communication path is a connectionless communication subnetwork. In other words, no prearranged communication path is established prior to the transmission of data. As a result, SNMP makes no guarantees about the reliable delivery of the data. Although in practice most messages get through, and those that don't can be retransmitted. The primary protocols that SNMP implements are the *User Datagram Protocol* (UDP) and the *Internet Protocol* (IP). SNMP also requires Data Link Layer protocols such as Ethernet or TokenRing to implement the communication channel from the management to the managed agent.

SNMP's simplicity and connectionless communication also produce a degree of robustness. Neither the manager nor the agent relies on the other for its operation. Thus, a manager may continue to function even if a remote agent fails. When the agent resumes functioning, it can send a trap to the manager, notifying it of its change in operational status. The connectionless nature of SNMP leaves the recovery and error detection up to the NMS (Network Management Station) and even up to the agent. However keep in mind that SNMP is actually transport independent (although original design was connectionless transport function, which corresponds to the UDP protocol) and can be implemented on other transports as well:

- TCP (Connected approach)
- Direct mapping onto Ethernet MAC level
- Encapsulation onto X25 protocol
- Encapsulation onto ATM Cell
- and so on.....

The following figure describes the Transport Mechanism used in SNMP over UDP:


Transport Mechanisms
Agent listens for message on UDP port 161
NMS
Network
SNMP Agent Protocol Engine
MIB
Agent
SNMP Protocol Data Units encapsulated within UDP datagrams

This protocol is carried by UDP. This connectionless protocol deliveries SNMP-PDUs without acknowledgements.

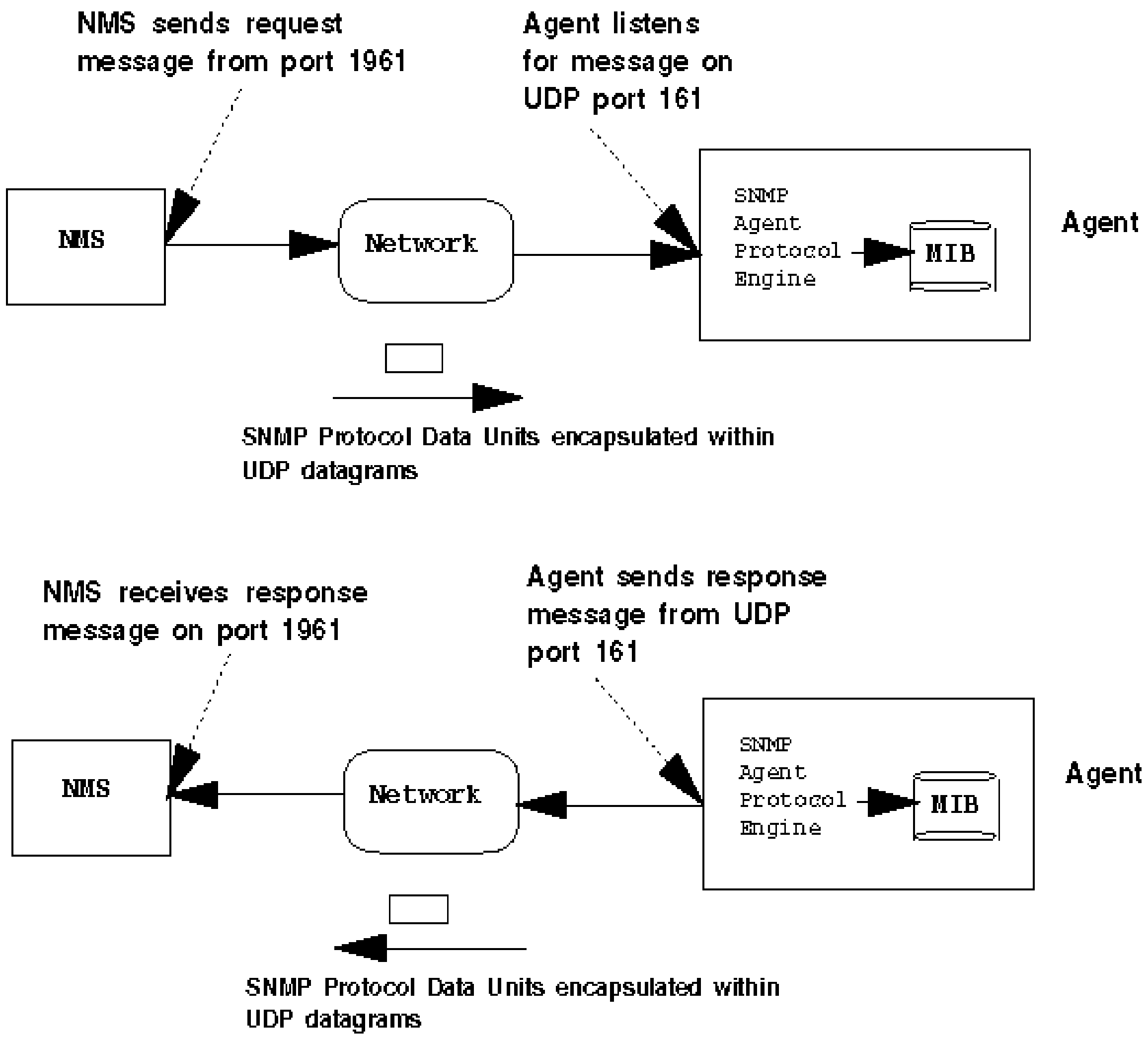
UDP Transport

- Agent listen on UDP port 161
- Responses are sent back to the originating NMS port from a dynamic port , although many agents use port 161 also for this target.
- Maximum SNMP message size is limited by maximum UDP message size (i.e 65507 octets)
- All SNMP implementations have to> receive packets at least 484 octets in length
- Some SNMP implementation will incorrectly or not handle packets exceeding 484 octets
- Asynchronous Traps are received on port 162 of the NMS

- UDP more suitable than TCP when dynamic route changes occur often (e.g. when there are problems in the network)
- UDP packets minimize the demands placed on the network (no resource tied up as with connection mode)
- Agent and NMS are responsible for determining error recovery. The following diagrams shows the architecture of UDP transport.

UDP Transport

Normal Send – Response Exchange


NMS sends request message from port 1961
Agent listens for message on UDP port 161
NMS
Network
SNMP Agent Protocol Engine
MIB
Agent
SNMP Protocol Data Units encapsulated within UDP datagrams
NMS receives response message on port 1961
Agent sends response message from UDP port 161
NMS
Network
SNMP Agent Protocol Engine
MIB
Agent
SNMP Protocol Data Units encapsulated within UDP datagrams

Outline of the SNMP protocol

Each SNMP managed object belongs to a “community”

- NMS station may belong to multiple communities
- A community is defined by a community name which is an OctetString with 0 to 255 octets in length.
- Each SNMP message consists of three components : a version number, community name, and data (a sequence of PDUs associated with the request)

Security levels with basic SNMP

Authentication

- trivial authentication based on plain text community name exchanged in SNMP messages
- authentication is based on the assumption that the message is not tampered with or interrogated

Authorisation

- Once community name is validated then agent or manager checks to see if sending address is permitted or has the rights for the requested operation
- "View" or "Cut" of the objects together with permitted access rights is then derived for that pair (community name, sending address)

Summary

- Not very secure
- SNMP version 2 is addressing this
- Extended security is possible with current protocol (example: DES and MD5)
- Does not reduce its power for monitoring

Structure of Managment Information

In the Manager/Agent paradigm for network managment, managed network objects must be logically accessible. Logical accessibility means that managment information must be stored somewhere, and therefore, that the information must be retrievable and modifiable. SNMP actually performs the retrieval and modification. The Structure of Managment Information (SMI) which is given in RFC 1155, is based on the OSI SMI given in Draft proposal 2684.

The SMI organizes, names, and describes information so that logical access can occur. The SMI states that each managed object must have a name, a syntax and an encoding. The name, an *object identifier*(OID), uniquely identifies the object. The syntax defines the data type,such as an integer or a string of octets. The encoding describes how the information associated with the managed objects is serialized for transmission between machines.

The syntax used for SNMP is the Abstract Syntax Notation One, ASN.1. The encoding used for SNMP is the Basic Encoding Rules, BER. The names used are object identifiers. later we will see how the MIB uses these names.

ASN.1 is used to specify many RFCs (and not just the SMI), for example the Internet standard MIB and SNMP. ASN.1 is used widely in OSI for specification purposes. ASN.1 used for defining SMI and MIBs is a subset of the ASN language given by OSI. ASN.1 does specify in itself

Object instances (protocol specific)
message transmission format (BER)

Click here to see more information on ASN.1 . Each object whether it's a device or a characteristics of a device, must have a name by which it can be uniquely identified. That name is the *object identifier*. It is written as a sequence of integers, separated by periods. For example, the sequence 1.3.6.1.2.1.1.1.0 specifies the system description within the system group, of the mgmt subtree.

The Internet Sub-tree

- Directory sub-tree if for future directory services
- Experimental sub-tree is for experimental MIB work - still has to be registered with the authority (IESG)
- Mib sub-tree is the actual mandatory Internet MIB for all agents to implement (currently MIB-II RFC 1156 - this is the only sub tree of mgmt)
- Enterprise sub-tree (of private) are MIBs of proprietary objects and are of course not mandatory (sub-tree registered with Internet Assigned Numbers Authority) for example: Cisco router OID: 1.3.6.1.4.1.9.1.1
- SNMP management nearly always interest in MIB and specific enterprises MIBs

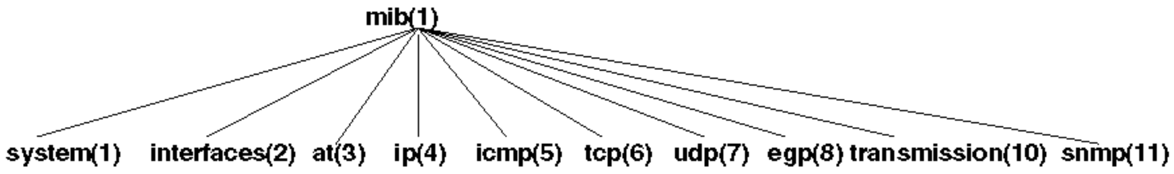
MIB-II Standard Internet MIB

- Definition follows structure given in SMI
- MIB-II (RFC 1213) is current standard definition of the virtual file store for SNMP manageable objects
- Has 10 basic groups
    - system
    - interfaces
    - at

  - ip
  - icmp
  - tcp
  - udp
  - egp
  - transmission
  - snmp
- If agent implements any group then is has to implement all of the managed objects within that group
- An agent does not have to implement all groups
- Note: MIB-i and MIB-II have same OID (position in the internet sub-tree)

MIB–II

The MIB Sub–tree



Note: There is an object cmot(9) under the mib but it has become almost superfluous and for all intents and purposes is not one of the SNMP manageable groups within mib.